AU/ACSC/109/2000-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

ORGANIZING TO WIN:

CENTRALIZED CONTROL FOR INFORMATION WARFARE

by

James Raley Marek, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: LtCol Jeffery R. Garner

Maxwell Air Force Base, Alabama

April 2000

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air Command and Staff College
Maxwell AFB, Al 36112

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Preface

While information has always been a component of warfare, only recently has information been addressed as method of, and target for, war. If we in the Air Force can claim our exploitation of the third physical dimension as a revolutionary advancement, certainly the our exploitation of information, a realm extending throughout the three physical dimensions of classical warfare, is even more so. Information warfare promises new frontiers for compelling an adversary to cede to our will—new capabilities, new vulnerabilities, and new ways of thinking about targets and effects, and perhaps even reality. To best employ information warfare, we must, in turn, structure ourselves to maximize its potential. This paper, then, is an attempt to look at the characteristics of offensive information warfare to determine how to best harness its nature.

I wish to thank ACSC for giving me the chance to think about a current issue, and then "encouraging" me to write about it. I am grateful for the guidance and indulgence of my research advisor, LtCol Garner. I thank my classmates, with whom I often discuss and debate ideas. To my children Ariece, Atlee, and Weston, I thank you for always being ready to play when Dad needed to "escape". I am especially grateful to my wife, Candy, for her support, and help. Finally, I thank God for my blessings—may I do your will always. It is my sincere hope that if war must come, what I have written will make the road to victory shorter and less costly, and the peace that follows longer.

Abstract

Information warfare promises to become a revolution in military affairs. If so, then not only must the technology adapted to military operations, but also organizations must adapt to bring the full capability to bear. This paper examines the nature of offensive information warfare and current doctrinally based organizational structures. Centralized control, linkages to intelligence, strategic capabilities, and security constraints are discussed. Based on these characteristics, alternatives to the existing framework are presented. Finally, recommendations are made for the framework of the information warfare organization of tomorrow.

Part 1

Introduction

Third Wave tools applied to a Second Wave organization deliver only a fraction of their potential. The military has barely begun to recognize this as an issue.

— Alvin and Heidi Toffler

A Revolutionary Wave

As the gates to the 21st century open, the dominating theme of every prognostication for the future includes the growth of and increased dependence on information and information systems. Indeed, Y2K was exclusively an information problem and the amount of money spent (up to one-half trillion dollars worldwide[1]) reflects the critical role information plays in our lives and well being—and our dependence continues to grow. As our dependence grows and as the criticality of our dependence increases, so too does our vulnerability. The U.S. is certainly the most vulnerable to information attacks (over twelve billion dollars spent last year on virus protection[2]), yet the awareness of our dependence and the availability of measures to protect this vulnerability increases the survivability of our systems against attacks. However, only through determined efforts at identification and implementation of protection measures for increasingly complex systems will the U.S. remain safe.

Satellites, cellular mobile service, cable, the telephone, and the Internet are creating multiplying paths of interconnectivity—powerful combinations that enable possibilities for

exploitation. There are new ways of doing business, new ways of committing crimes, and new ways of fighting wars—the emergence of the "third wave" according to the Tofflers.[3] GPS, smart bombs, sensor fuzed weapons, fire and forget missiles, AWACS, JSTARS and UAVs all reflect the growing importance of information-in-war. Furthermore, jamming, PSYOPS and leaflet drops represent the nascent capabilities of information warfare. The difference is subtle: Information-in-war refers to the application of increasing quantities of information to enhance or evolve existing capabilities. In information warfare, information can be a weapon and often, information is the target.[4]

It appears then, that the military has a new arrow in its quiver. Indeed, as information and information processing has had such a dramatic impact on the culture at large, many are predicting that the information revolution will enable a revolution in military affairs (RMA).[5] Certainly Desert Storm and more recently, operations in Kosovo have demonstrated the increasing role of information in military operations. If there is an RMA occurring before our eyes, we should see all four of the classic signs of successful adoption: new technology, military utility demonstrated, operational incorporation, and organizational restructure.[6] Examples of the first two have already been mentioned. Whether operational incorporation is occurring is unclear (secrecy inhibits level of incorporation) but certainly organizational change, as the epigraph suggests, has been slow in coming. Adaptations such as the Joint Forces Commander (JFC) Information Operations (IO) Cell or assignment of computer network attack to U.S. Space Command (on 1 Oct 2000[7]), among others, show movement, but none is the wholesale restructuring that an RMA seems to call for.

Information warfare easily has the potential to become an RMA. It is not only a new capability to enhance the effectiveness of today's weapons,[8] it is also a new way to fight, a new

way to mold the will of the adversary's populace, and a new way to shape the decisions of their political leadership.[9] Furthermore, this can be done without the use of any land, sea, or air forces. What if the U.S. could have convinced Sadaam Hussein that his Republican Guards had all surrendered, that his other forces had deserted, that his Scuds were inoperable, and that his only hope for survival was surrender? What if he did decide to surrender without a shot being fired? This is the possibility (not promise) of information warfare—the capability to more directly attack the will to fight, in addition to the capability to resist. If information warfare can indeed singularly attain operational and strategic objectives, then one might expect that something so important would have a new organizational structure, along with new professionals trained to use it, and new doctrine to implement it. If the military can fully adapt to information warfare, it would truly accomplish a revolution in military affairs, and perhaps enable continued US military success for decades to come.[10]

Is the Military Ready?

This paper assumes that the ubiquitous spread of information transmission and storage systems throughout the world, and most importantly, to those who wish to oppose us, presents new (if not revolutionary) opportunities for accomplishing our objectives. These opportunities include the ability to target information and information systems with information alone—a capability that only recently can lay claim to strategic (and even life-threatening) effects.

Yet, as this paper will show, the US military is not yet properly organized to employ the full capability of IW. The organizational adaptations to accommodate IW (as described in doctrine) are ad hoc and ineffective. A new organizational structure must be employed.

This paper, then, examines the question of how to organize joint forces to enable effective conduct of offensive information operations, and specifically strategic offensive information operations.[11] It will not address the legality or desirability of conducting information, nor will it progress beyond mere acknowledgment of the technical and intelligence requirements for conducting a successful campaign. It will assume that strategic offensive IW capabilities will or do exist and attempt to determine how to organize to best employ them.

This paper will first define and characterize strategic offensive information. Appropriate principles are developed to guide and support the eventual analysis of various organizational approaches. The existing organizational structure (as suggested in Joint and AF doctrine) and alternatives are then described and analyzed. Finally, the results of the analysis are organized to provide directions for the best approach.

It is only with wisdom that we are able to plan and act, instead of react. This paper, if successful, is the first step—extending the realm of knowledge with the hope of enabling wisdom. With a vision for what is possible, and the wisdom to act, we are best ready for what lies ahead.

Notes

[1] Jared Sundberg, "Why Y2K Won't Die," *Newsweek*, 10 January 2000, n.p.; online, Internet, 22 March 2000, available from http://newsweek.com/nw-srv/printed/us/sr/a47027-2000jan2.htm. See also "Experts: Y2K billions may pay dividends in the long run," *CNN*, 3 January 2000, n.p.; online, Internet, 22 March 00, available from www.cnn.com/2000/TECH/computing/01/03/y2k.long.term/index.html, and Dominique Deckmyn, "De Jager defends Y2K hype," *CNN*, 4 January 2000, n.p., online, Internet, 25 March 2000, available from www.cnn.com/2000/TECH/computing/01/04/dejager.y2k.idg/index.html. In Carolyn Duffy Marsan, "Y2K figures hide hardware upgrades," *CNN*, 10 January 2000, n.p.; online, Internet, 22 March 2000, available from www.cnn.com/2000/TECH/computing/01/10/y2k.budget.idg/index.html, John Koskinen, the US "czar" for Y2K, estimates $200 billion was spent world-wide on Y2K. The article also indicates "a lot of the money went for equipment upgrades that had little to do with Y2K compliance."

Notes

[2] Brian Forseca, "$12.1 billion reportedly spent to ward off computer viruses in 1999," *CNN*, 18 January 2000, n.p.; online, Internet, 25 March 2000, available from www.cnn.com/2000/TECH/computing/01/18/virus.cost.idg/index.html.

[3] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown and Company, 1993), 33-79. The first wave (of wealth generation and consequently, of war-making) is based on agriculture and the second, industry (mass production). The third wave is based on information or knowledge.

[4] Jeffrey R. Cooper, "Another View of Information Warfare: Conflict in the Information Age," in *The Information Revolution and National Security: Dimensions and Directions* ed. Stuart J.D. Schwartzstein (Washington, D.C.: The Center for Strategic and International Studies, 1996), 115. Cooper notes information can be described as a realm (environment), a resource, or a catalyst. While the "realm" definition most directly supports the premise presentated in this paper, the alternative perspectives do not change the argument presented here.

[5] For examples, see the first five articles (Part I) of *In Athena's Camp: Preparing For Conflict in the Information Age*, RAND Report MR-880-OSD, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), 23-171.

[6]Jeffrey R. Cooper, "Another View of the Revolution in Military Affairs," in *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND Report MR-880-OSD, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), 116.

[7] Ralph E. Eberhart, "Statement of General Ralph E. Eberhart, USAF, Commander-In-Chief North American Aerospace Defense Command and United States Space Command Before the United States Senate Armed Services Committee Strategic Subcommittee," *U. S. Space Command, Articles, Speaches, and Testimony by Key Individuals,* 8 March 2000, n.p.; online, Internet, 25 March 2000, available from http://www.peterson.af.mil/usspace/cinc8mar00.htm.

[8] Enhancing existing capabilities is not generally considered a revolution. An RMA should enable "new functions or meet previously unidentified requirements." Norman C. Davis, "An Information-Based Revolution in Military Affairs," in *In Athena's Camp: Preparing For Conflict In The Information Age*, RAND Report MR-880-OSD, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), 81.

[9] Martin Libicki and Jeremy Shapiro, "Conclusion: The Changing Role of Information in Warfare," in *The Changing Role of Information in Warfare*, RAND Report MR-1016-AF, ed. Zalmay M. Khalilzad and John P. White (Santa Monica, Calif.: RAND, 1999), 451.

[10] Cooper, "Another View of Information Warfare: Conflict in the Information Age," 126-128.

[11] This paper avoids defining information warfare in overly broad terms. John Rothrock notes the difficulty of defining that which is "*implicit* to all human endeavor, including warfighting [italics in original]." By focusing on a relatively narrow range of new or possible strategic offensive IW capabilities, this paper avoids the issues he addresses in his article. John Rothrock, "Information Warfare: Time for Some Constructive Criticism?" in *In Athena's Camp: Preparing For Conflict In The Information Age*, RAND Report MR-880-OSD, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), 220.

Part 2

Strategic Offensive Information Warfare

Wouldn't it be advantageous to find new ways to persuade the Milosevics of the world to negotiate, allowing NATO and the United States to withhold the use of their war machine in the first place and thus not having to deal with the technological problem sets of such a conflict?

— Timothy L. Thomas, "Kosovo and the Current Myth of Information Superiority"

Entice [the enemy] with something he is sure to take, and with lures of ostensible profit . . . await him in strength.

— Sun Tzu

Introduction

One could easily argue that information warfare is as old as warfare itself.[1] Many have noted that in the Civil War, commanders employed deceptions, balloons hoisted observers, troops cut telegraph lines—these and more can all be considered examples of information warfare (IW). Articulating what is new about IW in recent discussions has not been easy. Furthermore, just the definitions themselves cause consternation. Information, information operations, and information warfare have been defined and redefined in Joint and AF doctrine over the past few years. Even today, the Air Force offers "clarification" to current Joint definitions.[2]

To concentrate on the truly revolutionary, this paper confines itself to a narrow subset of what others may define as IW, specifically, strategic offensive IW. This section first describes

what is and is not strategic offensive IW in terms that are broad enough to lie within current Joint and AF definitions, yet specific enough to scope characterization. This section then describes organizational characteristics that are necessary for the effective exploitation of strategic information warfare capabilities.

Strategic Offensive Information Warfare (SOIW) Defined

Information operations (IO) are defined in Joint doctrine as "actions taken to affect adversary information and information systems while defending one's own information and information systems" at all times—peace or war.[3] This paper will use the Air Force definition of information warfare (IW): "information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems."[4] As shown in Figure 1, IW can be divided into two categories, defensive and offensive. Defensive IW involves the protection of friendly information and information processing systems from information attack.[5] Offensive IW attacks the adversary's information or information systems. It includes the alteration, creation, and deletion of an adversary's information or the degradation, disruption, destruction, or modification of his information systems to achieve a Joint Force Commander's (JFC's) objectives. Note that information attack is an offensive information warfare activity "taken to manipulate or destroy an adversary's information or information system without necessarily changing visibly the physical entity within which it resides.[6]

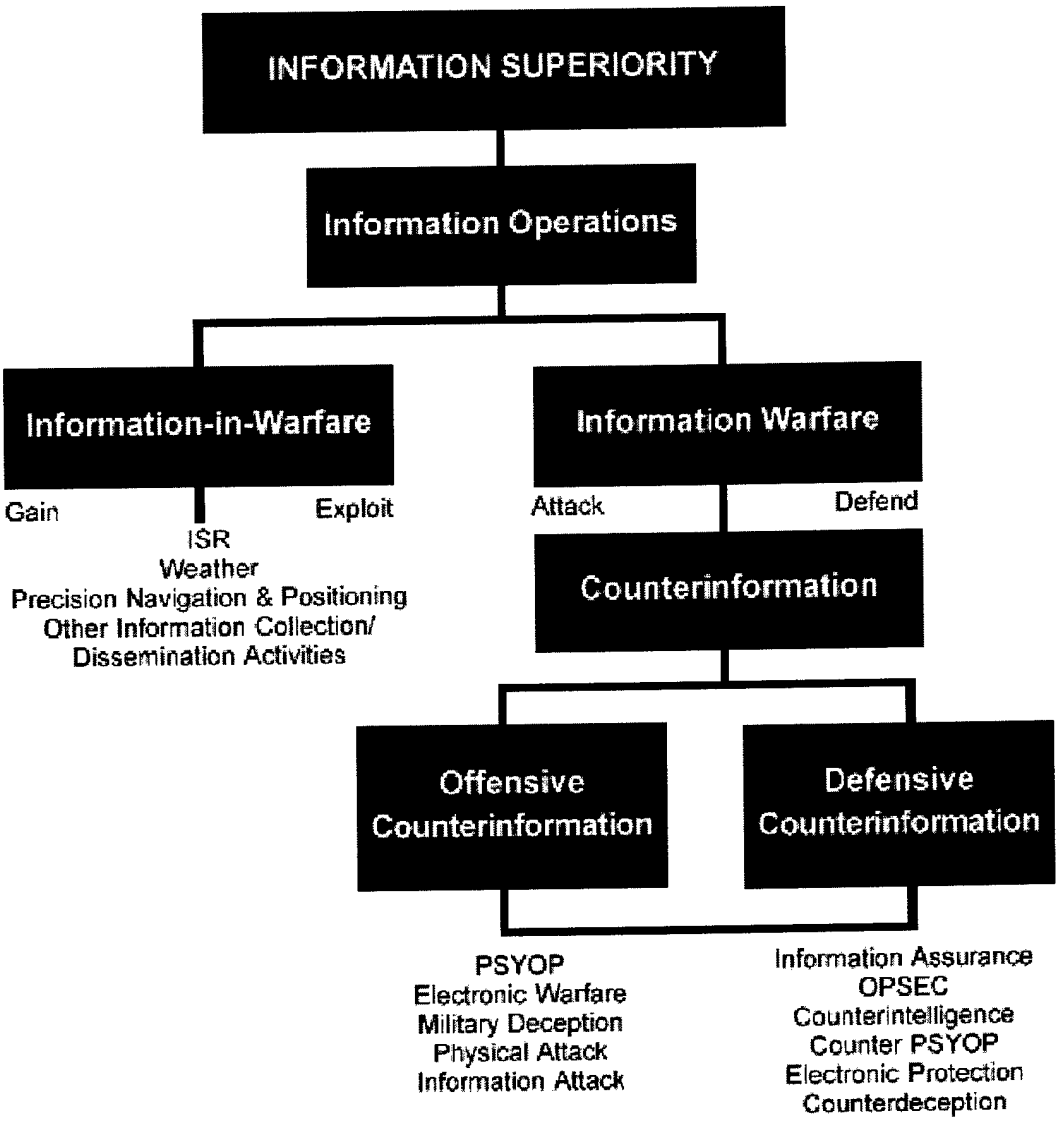

Figure 1 Air Force Approach to the Information Domain[7]

Offensive information warfare is the employment of the information instrument of power to achieve national objectives in time of war. Offensive information warfare uses the exploitation, or his access to information to achieve objectives. Aspects of command and control warfare that focus on the use of information (vice physical effects—bombing antennas, cutting wires, etc.) are included in information warfare.

Tactical information warfare only affects actions in the immediate battlefield area. Camouflage, displaying dummy vehicles, loudspeakers broadcasting a message of mercy for those that surrender—these are all examples of tactical information warfare. In the past 50 years, information warfare has surged through the electromagnetic spectrum. A communications jammer or a B-52 employing radar spoofing—to cause an air-to-air missile to explode prematurely—are both tactical forms of information warfare. Stealth technology, too, is tactical information warfare—it seeks to deny the enemy the ability to easily locate aircraft, ships, etc. (usually with radar, but IR, acoustic, sensors as well). Since tactical information warfare is (and has been) inextricably linked to military operations, its practices and utility are well understood. This paper will therefore focus on the strategic application of information warfare.

Strategic offensive information warfare (SOIW)[8], on the other hand, is aimed not at individual weapon systems or units, but at entire populations, entire armed services, and the leadership (of the military or country) of the adversary. Any information path that they use to form opinion or rely on to make decisions is subject to attack by IW in an attempt to end the war and achieve peace. Television broadcasts are one way to seek to influence the population of an entire nation—disrupting phone or electrical service is another. But strategic level campaigns need not be spread across a target of several millions. Indeed, from an economy of force standpoint and from a targeting importance standpoint, the focus of a strategic information warfare campaign is the enemy leadership.[9] Not only is this a smaller target (one to perhaps a few hundred), but it is also a target which, if properly handled, can directly affect the outcome of a war. **In this paper, therefore, strategic offensive information warfare (SOIW) is aimed at convincing the leadership that the initiation or continuation of hostilities is to their disadvantage, primarily (though not exclusively) through information attack.**[10]

Requirements for Effective Employment of SOIW

Congruence of Objectives

In any military endeavor, it is imperative that all operations at the tactical level support the tactical objectives. These tactical objectives should support the operational strategy, which should achieve the operational objectives. In turn, these should support the theater strategy, which should achieve the military strategic objectives. While tactical operations and objectives may differ markedly from one military unit to the next, they should all support the attainment of the military strategic objectives. In this respect, information warfare is no different from any other form of war—it, too, should seek congruence from the tactical to the strategic level of war.

Unity of Command

One of the foundational principles of war is unity of command. Unity of command is the admonition to focus resources and energies onto the main objective under the leadership of one commander. Note that joint doctrine understands that the separate services operate on different objectives and acknowledges that one person (in the form of the Joint Forces Commander) may not be able to command the massive military capabilities that may be required. It therefore, permits the delegation of control along component (service or functional) lines. These lines have generally clean boundaries (land, sea, air) and separable (yet coordinated, if not integrated) objectives. Given direction from the Joint Forces Commander, each component employs and controls its capabilities separately, but all work toward common strategic military objectives.

Security

Security is critical to the effective employment of offensive information warfare. If the enemy knows what is susceptible, what is vulnerable, what is questionable, then the effectiveness

of these techniques is diminished. Therefore, IW capabilities must be kept secret and unacknowledged with adherence to strict need-to-know. Separate capabilities should be held in separate channels. However, those planning the IW campaign require knowledge of all the available techniques so that they can synergistically employ the entire capability.

In the traditional military operations community, if a capability is compromised, then the adversary gains the opportunity to counter that capability. This usually takes time. During this period, by observing the adversary, the opportunity exists to discover that a capability has been compromised, to learn that the adversary is developing a counter capability, and perhaps even to determine the capabilities of the counter. In the SOIW, where the target may be the adversary's mind, if a capability is compromised, the adversary may not need to take any action at all. In the case where the counter to information is information, there is no development time, and little opportunity or "signature" that the capability has been compromised.[11] While the loss of capability may be the same as the traditional military case, discovering, assessing, and compensating for the loss can be much more difficult. It is the vulnerability of offensive information warfare, the ease of countering, and the difficulty of detecting a compromise that requires effective security.

The need for collaboration

While the enemy must be denied knowledge of IW activities and operations, individuals in U.S. intelligence services need to know what is going on in order to be able to report a complete, accurate intelligence picture. Otherwise, they too might be taken in by the "story" generated by offensive information warfare.[12] Therefore, in every intelligence collection discipline, there must be a mechanism to filter information that is collected on the adversary and flag, adjust, or maybe delete those "facts" which are a direct result of our information warfare activities. That way, they

can ensure that intelligence customers understand the true state of affairs, as well as the one generated by the influence of offensive information operations. A comparison of the two "versions" would also give an indication of the effectiveness of the information warfare campaign. Since only a few people would know the complete truth, a process and organizational structure must be put in place to track the collection as reported and the truth, and keep both sets of books in synchronization. Otherwise, for example, targets may be nominated (or fail to be nominated) based on information collected that reflected reality as altered by offensive information warfare operations. The wrong targets would be attacked while targets requiring attack escape unscathed. Therefore the organization must enable close contact, cooperation, and even adjudication between the information warfare operators and the intelligence collectors.

Summary

In order to understand how to organize for strategic offensive information warfare (SOIW), one must first understand the nature of information warfare. Information warfare has both offensive and defensive components. It can create effects at tactical level of war up to the strategic level. To be effective, offensive information warfare, like other forms of warfare, requires congruence of objectives, unity of command for best effect, security to protect its fragile capabilities, and close collaboration with intelligence to prevent feedback. Understanding these characteristics guides the examination of organizational structures to follow.

Notes

[1] Jeffrey R. Cooper, "Another View of Information Warfare: Conflict in the Information Age," in *The Information Revolution and National Security: Dimensions and Directions*, ed. Stuart J.D. Schwartzstein (Washington, D.C.: The Center for Strategic and International Studies, 1996), 112.

Notes

[2] Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 5 August 1998, 41-42.

[3] Joint Publication (Joint Pub) 3-13. *Joint Doctrine for Information Operations*, 9 October 1998, GL-7.

[4] AFDD 2-5, 42.

[5] Defensive information warfare is a current topic of high interest, further heightened by the Y2K episode. While not information warfare, the Y2K "scare" revealed glimpses of our vulnerabilities to disturbances in information systems and generated a significant amount of interest in protecting them. Unfortunately, as time passes and in the absence of any other "attack", this interest will most likely fade. For now, however, there exists a significant body of literature on this subject—therefore defensive information warfare will remain outside the focus of this examination. But since some of the very same techniques used for our offensive information warfare may be used against us and must be defended against, there is then a need to have offensive and defensive information warfare organizations joined at the hip. This idea is presented in Appendix C of this paper.

[6] AFDD 2-5, 15.

[7] AFDD 2-5, 3.

[8] I define SOIW, then, as a subset of information operations (IO) and information warfare (IW). It is specfically not information-in-warfare(IIW).

[9] This definition maintains congruence with Joint Doctrine, but Joint Doctrine is not always clear—especially for information operations. Compare the statement "offensive IO for strategic level objectives seek to engage adversary or potential adversary leadership to deter crisis and end hostilities once they occur" with "offensive IO at the operational level of war will focus on an adversary or potential adversary in the combatant commander's AOR. These offensive IO focus on maintaining peace, deterring crises, and, failing deterrence, on supporting quick resolution of hostilities on terms favorable to the United States" (both Joint Pub 3-13, II-10). The objectives are the same—the difference is "leadership". This paper includes effects on leadership, therefore it must address the strategic level. This does not exclude the application of similar arguments to operational level organizational issues.

[10] Jeremy Shapiro, "Information and War: Is it a Revolution?" in *The Changing Role of Information in Warfare*, RAND Report MR-1016-AF, ed. Zalmay M. Khalilzad and John P. White (Santa Monica, Calif.: RAND, 1999), 144 and Richard Szafranski, "Neocortical Warfare? The Acme of Skill," in *In Athena's Camp: Preparing For Conflict in the Information Age*, RAND Report MR-880-OSD, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), 404-405.

[11] Suppose the enemy learned of US IW activities against him. He need do nothing. When data came in through channels he knows are compromised, the adversary might discount the reports, rather than believe them at face value. The US might never know that this compromise has occurred and assume that the adversary is completely convinced. The enemy is using information to counter (in the battle for the decisions he makes) US information, and the US is none the wiser. It could be argued that his lack of trust in the reports accounts for partial success in the IW operation, but since the US was not able to get him to take the reports as truth, the effect is less that expected.

Notes

[12] Peter D. Feaver, "Blowback: Information Warfare and the Dynamics of Coercion," *Security Studies* 7, no. 4 (Summer 1998): 104-107.

Part 3

Organizational Analysis

> *the conduct of integrated information operations was hampered by the lack of advance planning and necessary strategic guidance to define key objectives . . . The Department will ensure that information operations planning is initiated early and synchronized with other operational plans.*
>
> — Kosovo/Operation Allied Force After Action Report to Congress, 31 Jan 00

Current Organizational Structure

Joint Doctrine organizationally incorporates Information Operations (IO) in the form of the IO planning cell (see Figure 2). This is a coordinating body composed of representatives from IO-responsible organizations and normally led by the J-3, but operationally supervised by the IO officer. The IO cell can notionally consist of representatives of eighteen organizations. These representatives accomplish the required planning and coordination of information operations.[1]

Clearly, this structure is a first-draft attempt to incorporate information warfare into existing warfighting and doctrine. In an analysis of Revolutions in Military Affairs (RMAs), Norman Davis notes "frequently, organizations try to fit the innovative technology into established ways of doing things, and these innovations are expected to prove themselves in terms of existing measures of effectiveness."[2] Although the intent behind the formation of the IO cell is laudable, the result is weak (as the epigraph suggests).

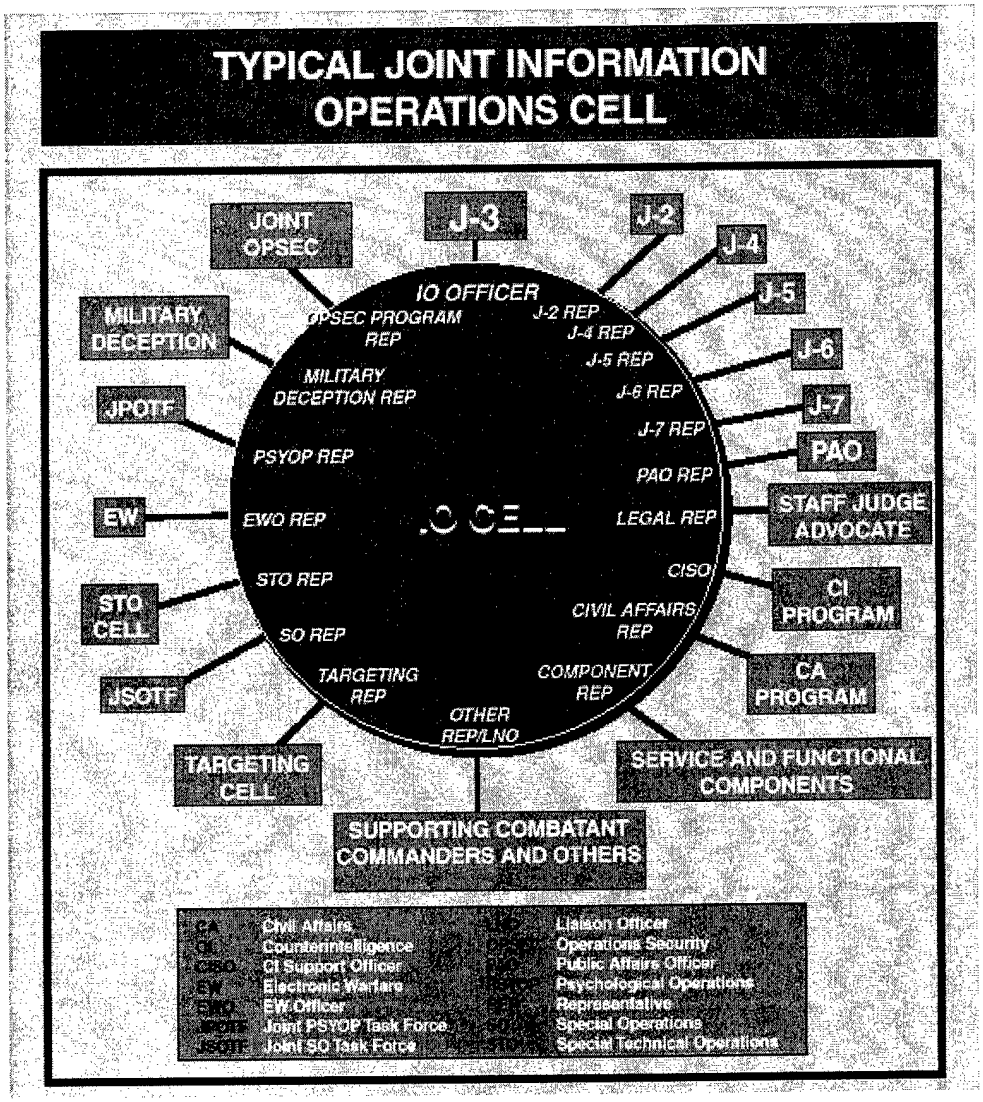

Figure 2 Typical IO Cell Organization[3]

In the IO cell, decentralized execution is preserved, but centralized control is reduced to "coordination". At best this is synchronization, and at worst blind deconfliction. Even theorists who are espousing networked organizational forms for the military acknowledge the benefits of "a central understanding of the big picture that enhances the management of complexity".[4] The IO cell falls far short of providing this sort of awareness or control.

This structure does not leverage the strategic capabilities of information warfare.[5] The J-3 is in charge of IO, and usually appoints an IO officer to supervise the IO cell—the IO officer "will ensure IO is implemented per the JFC's guidance. This may entail . . . directly facilitating coordination between the components or staff organizations responsible for planning and execution of IO."[6] The fact the organization is a planning and coordination cell is a good indicator that the organization lacks significant influence. Furthermore, IO leadership is a mid-level staff officer. His IO issues face an uphill battle against the desires of a much more senior component commander.

Congruence of Objectives

While Joint doctrine provides examples of IO objectives, it is unclear on who determines them. The IO cell does not appear to be responsible, yet it is the JFC's primary source of expertise on the subject. In fact, no mention of the IO cell is made in any direct or supporting role in determining IO objectives. The only other source of expertise, then, is in the components. If left up to the components, the IO objectives will almost certainly end up in direct support of those components' objectives, and neglect to leverage the full impact of IO capabilities. Without clarification, it appears that the lack of clear responsibility precludes the establishment of sound IO objectives, at either the strategic or operational level. Without higher level IO objectives established by those knowledgeable, IO objectives at the lower level are at best supportive of land, sea, and air objectives—not IO objectives. This results in up to three separate approaches and sets of operational objectives assigned to informational concerns, all in support of notional strategic informational objectives (if they even exist at all as a separate entity—if not, then they support the existing warfighting strategic objectives). So doing presents a stove-piped approach for information warfare, one that must be brought into congruence at the strategic level by the

JFC. Without building from the bottom-up, attempts to force congruence become cumbersome, with top-level pressure, rather than bottom up initiative. This subjugates information to achieve, at best, component level (read operational or even tactical) level objectives. Furthermore, with a lack of congruence in the strategic level informational objectives, aspects of one component's tactical information operation may contradict those of another component. This incongurency remains hidden when components are allowed to focus their IO on self-supporting goals and objectives. The fact that the IO cell serves as deconfliction center highlights the fact that the information operations of separate components may serve different (if not cross) objectives.

Unity of Command

As discussed earlier, strategic offensive information warfare (SOIW) can achieve strategic effect separate from land, sea, or air, yet the people that directly execute IO capabilities are land, sea, or air component commanders (or service component commanders). While the IO cell does plan an IO campaign for the JFC, it does so based on capabilities offered by each service. Upon employment, each service carries out its plan according to its own doctrine. Certainly the IO cell can provide deconfliction, but given the precision and integration that future IW capabilities will require, this will certainly limit effectiveness. These commanders will tend to employ IO capabilities to achieve objectives directly pertaining to their own core competencies—objectives that they already played a major role in determining. Even if there existed overarching IO objectives, the commander is most likely going to side with his own objectives, rather than support IO objectives determined outside the component. Such is result when unity of command is violated.

Security

The IO cell can be strong at security. As a deconfliction organization, only the minimum amount of information needs to be exchanged. However, it is unclear to what extent information defenders need to be involved in offensive operations. It would appear that by combining offensive IO and defensive IO in one organization, the security principle of need-to-know could be easily violated.

Collaboration with Intelligence

By merely providing a coordinating function, the linkages between IW and intelligence are weak. A single person (the J-2 representative) is unable to monitor all ongoing information operations with the level of detail needed to properly filter intelligence reporting and screen or flag assessments that have been influenced by IW attacks on the adversary. This lack of integration represents a significant risk of misreading adversary capabilities and intentions to the degradation of the entire (not just the IW) campaign.

Organizational Alternatives

Networked

Networked organizations employ the expertise of dispersed elements of the organization by leveraging real time communications, rather than gathering the elements at one location. The first contemporary use of networked organizational structures in wartime occurred in the Gulf War. The Gulf War Air Power Survey notes "the prevalence of such organizations [in the Gulf War] may prove part of a broader trend and not merely an aberation."[7]

In a networked approach, SOIW capabilities are spread throughout the services, the U.S. Government, and perhaps even industry. As required capabilities are identified, they are

employed where they reside (or purchased—"just in time"). This approach highlights and maximizes the "in-place" nature of information warfare and leverages its strengths. It also presents a tougher target for an adversary. Dispersed operations can enable more access points (to different networks—cell, internet, phone, satellite) than any one location. Unfortunately, dispersal creates more difficulties for security (larger perimeter, protection of communications, etc.)

Even in a networked organization, the nature of the military requires that one must still have leadership, accountability, responsibility, and authority. Therefore, a networked organization must recognize and incorporate the centralized control of a commander, while enabling the decentralized execution of functions or duties.

Indeed, even if not a desirable final solution, it is possible that this organization structure may be a future, and perhaps even likely, transition on the road to an empowered organizational structure.

Place in Special Operations

In this proposed construct, information warfare capabilities are placed under USSOCOM. Perhaps separate from the Navy, Army, or AF components, or perhaps contained within one, strategic information warfare is blended with PSYOP and similar capabilities already existing in special operations. As USSOCOM capabilities are employed in the entire spectrum of operations from non-combatant evacuation operations (NEOs) to full-scale wars, information warfare is an organic capability that can enable success.

Special operations focuses on tight security; distinct, discrete missions; and employing a small cadre of highly trained personnel to carry them out. These characteristics are well suited to information warfare. Today, it is difficult to see a future where SOIW attacks are launched by

teams of "shooters" located all across the United States and in theater. Instead, one pictures a single room or perhaps two, filled with computers and communications equipment, with 30-50 people engaged in information warfare. These are the sorts of numbers suited for special operations.

While special operations provides a the right environment to employ IW in support of limited, focused operations, it is not clear that special operations would serve as the best host to a full scale information campaign. The idea of an entire operational campaign being waged by young troops typing at a keyboard may not fit their image—indeed, it may detract from other "special" capabilities that only special operations can perform.

Component

In this idea, information warfare is structured as a distinct warfighting component. This leverages the full capabilities of information warfare, provides for the proper interfaces, and enables an appropriate level of centralized control. A joint forces information component commander (JFICC), as a functional commander-in-chief (CINC), would maintain "combatant" command over all assigned information warfare capabilities and personnel.[8] Some of these may be chopped to other commanders for operational and tactical engagements, but the bulk of his force will be employed to achieve the strategic and operational informational objectives as set by the JFC (with his input). In peacetime, most of his forces may be assigned to other duties or commands. However, he and his staff would be responsible for the development of planning and budgeting for SOIW needs.

Space may be a good example. It is recognized that space is important enough to enjoy its own unified command and its own CINC. Even while often subsumed as part of aerospace

power, space enjoys some sense of independence and autonomy. Interestingly enough, space is hosting increasingly greater responsibilities in information operations.[9]

Many oppose the creation of an information warfare component along with its inherent functional component commander. It is cited that a JFICC would own or task air and space information assets already assigned to the joint forces air component commander (JFACC) (JSTARS, AWACS, U-2s, etc). This violates unity of command, as well as simplicity.[10]

The distinction made in this study is that of the operational/strategic level of war and information warfare versus the tactical level of war and information-in-war. AWACS and JSTARS provide real time views of a battle—certainly taking tactical pictures that are exploited to enable tactical (and eventually operational) success. Furthermore, these are examples of information gathering assets enhancing air/land/sea operations—information-in-war. The JFICC described in this paper is not focused on these capabilities—he is looking at strategic offensive information warfare (and perhaps information protection). His focus is on operational and strategic effects, not tactical information supporting standard operations.

Combining with Intelligence

One particularly interesting structure is to combine information warfare capabilities with intelligence. Both work with almost exclusively with information. Action by one has a direct and substantial effect on another. Offensive information warfare and intelligence form a loop of information flows and effects. The complement is defensive information warfare, which, along with counterintelligence, seek to block (from our perspective) information flows in the opposite direction. The symmetric construct provides mutual support and combines like functions.

Of course, all of the services require intelligence. Bringing together information and intelligence might seem to reducing the effectiveness of the information gathering capability of

the services themselves. However, there are constructs that still protect not only the services extant intelligence capabilities but also a large fraction of their current intelligence personnel as well. This might be just a consolidation with current intelligence analysis and production. Perhaps this is a DIA-level consolidation. DIA could become the Defense Information Agency. It would provide each CINC Intelligence/IO teams led by a senior military commander (who could function as a JFICC). The intelligence side of the team could be led by a dual-hatted J-2. He continues to provide intelligence estimates to the JFC, who then tasks his component commanders (including the JFICC) with operational guidance.

This pairing helps negate the corruption of one's intelligence by the (uncoordinated) application of offensive information warfare.[11] Those who are watching and listening to the adversary are working hand in glove with those who are, perhaps surreptitiously, influencing what the adversary sees and hears. Furthermore, closely related aspects of intelligence and information warfare (such as the lines between counterintelligence and defensive information warfare) can be clearly defined and duplication eliminated if both groups are under one roof.

Summary

Current doctrine provides for coordination of information operations via the IO cell. Unfortunately, it is incapable of providing the focus and direction necessary to accomplish strategic offensive information warfare objects (in Kosovo, even less). A sampling of alternative organizational approaches demonstrates the wide range of possibilities—each offering substantial improvement over the current structure.

Notes

[1] Joint Publication (Joint Pub) 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, IV-3.

[2] Norman C. Davis, "An Information-Based Revolution in Military Affairs," in *In Athena's Camp: Preparing For Conflict In The Information Age*, RAND Report MR-880-OSD, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), 81.

[3] Joint Pub 3-13, IV-3.

[4] John Arquilla and David Ronfeldt, "Cyberwar is Coming," in *In Athena's Camp: Preparing For Conflict In The Information Age*, RAND Report MR-880-OSD, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), 31-32, 45.

[5] IW commenter John Rothrock notes, "The best technology, even when employed with the greatest of tactical effectiveness, can be counterproductive if the technology and its employment are not orchestrated against a set of well conceived, hierarchically consistent operational, strategic, and policy objectives. While this observation is true regarding any military or quasi-military undertaking, it is especially important regarding Information Warfare which is first and foremost an intellectual rather than a technological or physical undertaking." The observations in this paper support his statements. John Rothrock, "Information Warfare: Time for Some Constructive Criticism?" in *In Athena's Camp: Preparing For Conflict In The Information Age*, RAND Report MR-880-OSD, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), 222.

[6] Joint Pub 3-13, IV-3.

[7] Thomas A. Keany and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report* (Washington, D.C.: U.S. Government Printing Ofice, 1993), 247-248.

[8] For different approaches on responsibilities, see Jeffery R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB, Ala.: Air University Press, 1996), 4 or see Dwayne W. Frye, "Information Warfare (IW): Air Staff Roles and Responsibilities," Research Report no. AU/ACSC/0603/97-03 (Maxwell AFB, Ala.: Air Command and Staff College, March 1997).

9 Ralph E. Eberhart, "Statement of General Ralph E. Eberhart, USAF, Commander-In-Chief North American Aerospace Defense Command and United States Space Command Before the United States Senate Armed Services Committee Strategic Subcommittee," *U. S. Space Command, Articles, Speaches, and Testimony by Key Individuals*, 8 March 2000, n.p., online, internet, 25 March 2000, available from http://www.peterson.af.mil/usspace/cinc8mar00.htm.

[10] See Jeffrey D. Seinwill, "Organizing Joint Forces for Information Operations: The Viability of a Joint Force Information Operations Component Commander," Research Report no. AU/ACSC/185/1999-04 (Maxwell AFB, Ala.: Air Command and Staff College, April 1999). Also see "Joint Force Information Warfare Component Commander," *HQ USAF Doctrine Center--Doctrine Issues, Initiatives and Information,* Feb 00, n.p.; online, Internet, 25 March 00, available from www.doctrine.af.mil/application/issues/jfiwcc.pdf.

[11] Peter D. Feaver, "Blowback: Information Warfare and the Dynamics of Coercion," *Security Studies* 7, no. 4, (Summer 1998): 104-107.

Part 4

Conclusions

In Washington it usually takes about two days to figure out what the problem is, about two months to figure out what a plausible solution is, and about two years to determine who actually implements it.[1]

— Michael Nelson

The ingredients for a transformation of war may well have become visible in the Gulf War, but if a revolution is to occur someone will have to make it.

Thomas A. Keany and Eliot A. Cohen, Gulf War Air Power Survey Summary Report

The biggest challenge is determining whether information warfare, like intelligence, is something so basic to the success of any service that it must be present as part of them all, or whether it is something much different than the services themselves—perhaps so different as to belong in its own Department of Information. Airpower has had similar concerns. Airpower is a key component of each service (the army has more airframes than the Air Force), yet it is still necessary, and arguably rightfully so, that the nation needs a separate air service, the Air Force. This is due not only to the unique qualities that airpower provides (the foremost being elevation, which all services leverage in some degree or another) but also the unique functions that airpower alone can accomplish. The Air Force is able to focus its effort on making maximum use of these functions to the better defense of our nation. Information warfare is similar to airpower in that is has unique qualities and capabilities—these may support or may even be a key

component of the services. But only when information warfare is substantially free to pursue and refine capabilities that are unique to its own, will we truly make the best use of this new way of waging war.

Unfortunately, the IO cell fails to employ information warfare capabilities in an effective manner—not due to a lack of effort, but due to its inherent organizational structure. Only through organizational change, will IW be employed effectively.

This paper presented several organizational alternatives and it is clear that there are desirable aspects of in each—the best approach may make use of different aspects of separate alternatives. Centralization is necessary for control, for planning, and for effect in order to realize the full capability of information warfare. Security and the independent strategic capabilities of information warfare also support this arrangement. Centralized control also indicates the need for a single, high-ranking person overseeing information warfare. This would facilitate interactions with the Joint Forces Commander, as well as provide senior leadership and perspective to forces from other services over which he may be assigned operation control.

The ability to wage warfare from any computer or from any phone does highlight a key capability if the need is apparent. While centers of excellence for Internet, cell phone, and satellite IW R&D may be separate, offense and defense oriented missions should be collocated. (The need to centralize offensive and defensive R&D is addressed in Appendix C.)

The need to tie IW and intelligence is also strong. These two functions work hand-in-hand. While this paper does not suggest that CIA, DIA, NSA, NRO, and IW combine to form a single IW/Intelligence entity, it does seem clear than when waging war (and when actively employing offensive IW capabilities), intelligence and IW need to be working as one team. Therefore, on the military side of intelligence, IW and intelligence must be tightly linked.

Collocation of the protection half of information warfare does not appear critical to the success of a strategic offensive information warfare campaign. Furthermore, protection can be considered a combat support function (similar to air base protection).

These findings are summarized as follows:

- The current IO Cell organizational structure is ineffective and should be replaced
- Centralized command and control of consolidated capabilities under a single individual is essential
- Close ties with intelligence gathering and production functions is necessary
- Secrecy points to centralization
- The offensive side of IW does not depend on collocation with the defensive half
- Several organizational options exist which achieve improvements over the existing structure

Closing

While current AF doctrine may be forward thinking in describing IO from a capabilities standpoint, it is short sighted in its organizational constructs. This paper recommends that the military begin to move IW away from a "cell" to coordinate capabilities, and towards centralizing capabilities under a single organization. In wartime, a single individual should be given command of these capabilities, and he should report directly to the JFC. Operationally this is the best way to bring IW to bear on the adversary.

What this paper cannot determine is where this organization should reside and at what level it should exist. Not only are these decisions political in nature, there is a breadth and depth to these questions that only a detailed study can attempt to explore. However, the examples

outlined in the previous section provide highlights of the range of possibilities and some of their strengths and weakness.

As the initial epigraph suggests, the easy work is now complete. A problem has been identified. Furthermore, plausible solutions have bee proposed to remedy the problem. What remains is the challenge of determining the future course, bringing the ship around, and traveling to a better destination. It will not be easy or simple, but it will be worthwhile. This author looks forward to witnessing, and perhaps even participating, in the journey.

Notes

[1] Michael Nelson, "The View from the White House: A Public Policy Perspective," in *The Information Revolution and National Security: Dimensions and Directions*, ed. Stuart J. D. Schwartzstein (Washington, D.C.: The Center for Strategic and International Studies, 1996), 66.

Appendix A

Future possibilities

In the future, information warfare may take on the characteristics of other forms of warfare, in that the target of information is information first, then other capabilities. In naval warfare, one must first obtain "command of the sea", before one effectively apply naval power to activities on land. In air warfare, one first seeks air superiority, before one takes on strategic bombing, interdiction, and close air support missions. Perhaps the same is true in information. One may need to target our offensive capabilities against the adversary's offensive capabilities first, then use our information control or superiority to accomplish other missions. If there is such as a phenomenon, then certainly the organization for information operations will not only reflect that of conventional warfare, it will also ascribe a level of importance comparable to those of the conventional armed services. This may even raise the possibilities of an information department coequal with Army, Navy, and Air Force.

Appendix B

Further Research

It is clear that how we are organized for information warfare is bound to change, is only a matter of how and when. This study, along with others preceding it, has laid out basic foundational elements. The building up and expanding on this work to a level of detail required for a decision-maker still remains.

As stated earlier, while this paper did recommend centralization of IW capabilities under a single commander, this paper deliberately did not address how to transition to these new organizational elements, and when the transitions should occur. Further research might look into the need and feasibility for a separate service or the approach for centralizing IW in its own command—since the later is a more near-term possibility, this would have the greatest payoff.

Another approach is to look at the current organizational structure as outlined in doctrine and look at past experience, as well as today's operations, and characterize the strong and weak areas. Recommendations based on an analysis of these results might provide a convincing argument for a specific organizational construct (including the one already in place).

The idea of combining intelligence and information warfare needs to be worked in greater detail. USSOCOM already combines IW and intelligence. A study of their approach, and how that might be translated into a JTF-wide implementation should provide valuable insight into a promising possibility.

An interesting side-note to this study might be a survey of military and public opinion on the legality, usefulness, and desirability of employing different types of information warfare—and comparing the responses. Tampering with bank accounts, turning off power, shutting down economic production capability, falsifying information to influence decision-makers, broadcasting false information—there are notional capabilities that a military might employ. How do people feel about employing them in a humanitarian operation, to convince a terrorist to turn himself in, or to avoid another Gulf War? Such a survey might reveal interesting trends on how far we might let information warfare capabilities develop—and even if we do develop them, the popular support may not exist to even allow them to be employed.

One particularly interesting aspect of information warfare is the lack (in contrast to land, sea, and air warfare) of a geographic characteristic. If we are attacked informationally by an outside entity, and we decide to respond militarily and specifically, informationally, who is the CINC? Is it Joint Forces Command or the CINC where the attack originated? What if it is not state sponsored? This is not necessarily an organization issue or an information warfare issue, but the responsibility does need to be determined.

Given the need for intelligence to become tightly linked to information-in-warfare and information warfare, a critical question is if we can combine intelligence and IW. How does it then support information-in-warfare? Intelligence is not operational from the military perspective. If made part of IW, it could either be coequal—giving an op and non-op activity equal status, or it could be subordinate to IW, and therefore less responsive to needs of other components.

Finally, this entire research is based on unclassified sources and is intended for generic military audiences. Unfortunately, this tends to water down the analysis. Depending on the

reception of this and further investigations, a classified study might be worthwhile. This would permit consideration of relationships, capabilities, budgets, etc. in order to provide concrete evidence for specific recommendations.

Appendix C

Organizing R&D

No matter what the structure for organizing offensive information warfare, it is clear that defensive information warfare has some of its own peculiar needs that drive its organization. Again, centralized control (to determine policy, identify vulnerabilities, and communicate fixes) and decentralized execution (each organization will have its own defensive information specialist to tailor fixes to their own systems) seem to make sense. Especially in defensive information warfare, the centralized control will be national in scope, with responsibilities extending from the public into the private sector. Whether this national entity is vetted in the department of defense is not a concern here—what is clear is that there will be some single organization or group responsible for information defense.

In information operations R&D, the tie between offense and defense needs to be extremely close. Any capability that is determined from an offensive standpoint needs to be defended against. Similarly, any vulnerability identified by the defenders as requiring protection should be a candidate for an offensive capability. Furthermore, information systems, based as they are on commercial markets, tend to align themselves along commercial standards. These standards encourage commonality in several respects—commonalties that may help enable exploitation of families of systems.

Based on these characteristics that the research and development of offensive and defensive information warfare capabilities, tactics, and techniques be tied closely together, if not collocated. Certainly in this nascent era of interconnectivity, one would argue that when discussing information warfare techniques, separation across the country is the same as separation across the cubical. I submit, however, that there is some additional benefit that might be realized from collocation—while I have yet to determine any operational advantage from geographic separation. Therefore, while operation employment of information warfare may be geographic independent, at this time, it seems advantageous to have offense and defense R&D working side by side.

Glossary

ACSC	Air Command and Staff College
AF	Air Force (United States Air Force)
AFIT	Air Force Institute of Technology
AU	Air University
AWACS	Airborne Warning and Control System
AWC	Air War College
C4I	Command, Control, Communications, Computers, and Intelligence
CADRE	College of Aerospace Doctrine, Research, and Education
CCAF	Community College of the Air Force
CIA	Central Intelligence Agency
CINC	Commander in Chief
DIA	Defense Intelligence Agency
DOD	Department of Defense
IA	Information Attack
IO	Information Operations
IW	Information Warfare
JFACC	Joint Forces Air Component Commander
JFC	Joint Forces Commander
JFICC	Joint Forces Information Component Commander
JFIOCC	Joint Forces Information Operations Component Commander
JFIWCC	Joint Forces Information Warfare Component Commander
JSTARS	Joint Surveillance Target Attack Radar System
JTF	Joint Task Force
NEO	Noncombatant Evacuation Operation
NRO	National Reconnaissance Office
NSA	National Security Agency
PSYOP	Psychological Operations
R&D	Research and Development
RMA	Revolution in Military Affairs

SOIW	Strategic Offensive Information Warfare
UAV	Unmanned Aerial Vehicle
USAF	United States Air Force
USSOCCOM	US Special Operations Command

Definitions

information attack. An activity taken to manipulate or destroy an adversary's information systems without visibly changing the physical entity within which it resides. (AFDD 2-5)

information-in-warfare. Involves the Air Force's extensive capabilities to provide gloval awareness throuthout the range of military operations based on integrated intelligence, surveillance and reconnaissance (ISR) assets; its information collection/dissemination activities; and its global navigation and positioning, weather, and communication capabilities. Also called IW. (AFDD 2-5)

information operations. Actions taken to affect adversary information and information systesms while defending one's own information and information systems. Also called IO. (Joint Pub 3-13) The Air Force offers the following for clarity: Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare. (AFDD 2-5)

information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Also called IS. (Joint Pub 3-13) The Air Force prefers to cast 'superiority' as a state of relative advantage, not a capability, and views IS as: That degree of dominance in the information domain which allows friendly force the ability to collect, control, exploit, and defend information without effective opposition (AFDD 2-5)

information warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW. (Joint Pub 2-13) The Air Force offers the following for clarity: Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems. (AFDD 2-5)

offensive counterinformation. Offensive IW activities which are conducted to control the information environment by denying, degrading, disruption, destroying, and deceiving the adversary's information and information systems. Also called OCI.

offensive information operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack. (Joint Pub 3-13)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (Joint Pub 1-02)

Bibliography

Air Force Doctrine Document (AFDD) 2-5. *Information Operations*. 5 August 1998.

Air Force Doctrine Document (AFDD) 2-1-2. *Strategic Attack*. 20 May 1998

Arquilla, John, and David Ronfledt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age*. RAND Report MR-880-OSD. Santa Monica, Calif.: RAND, 1997.

Arquilla, John and David Ronfeldt. "Cyberwar is Coming." In *In Athena's Camp: Preparing For Conflict In The Information Age*. RAND Report MR-880-OSD. Edited by John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND, 1997.

Barnett, Jeffery R. *Future War: An Assessment of Aerospace Campaigns in 2010*. Maxwell AFB Ala.: Air University Press, 1996.

Cooper, Jeffrey R. "Another View of Information Warfare: Conflict in the Information Age." In *The Information Revolution and National Security: Dimensions and Directions*. Edited by Stuart J.D. Schwartzstein. Washington, D.C.: The Center for Strategic and International Studies, 1996.

Cooper, Jeffrey R. "Another View of the Revolution in Military Affairs." In *In Athena's Camp: Preparing for Conflict in the Information Age*. RAND Report MR-880-OSD. Edited by John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND, 1997.

Davis, Norman C. "An Information-Based Revolution in Military Affairs." In *In Athena's Camp: Preparing For Conflict In The Information Age*. RAND Report MR-880-OSD. Edited by John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND, 1997.

Dominique Deckmyn. "De Jager defends Y2K hype." *CNN*, 4 January 2000, n.p. Online. Internet, 25 March 2000. Available from www.cnn.com/2000/TECH/computing/01/04/dejager.y2k.idg/index.html.

DiCenso, Major (Retired) David D. "IW Cyberlaw: The Legal Issues of Information Warfare." *Airpower Journal* 13, no. 2 (Summer 1999): 85-102.

Eberhart, Ralph E. "Statement Before the United States Senate Armed Services Committee Strategic Subcommittee." 8 March 2000, n.p. Online. Internet, 26 March 2000. Available from http://www.peterson.af.mil/usspace/cinc8mar00.htm.

"Experts: Y2K billions may pay dividends in the long run." *CNN*, 3 January 2000, n.p. Online. Internet, 22 March 00. Aavailable from www.cnn.com/2000/TECH/computing/01/03/y2k.long.term/index.html.

Feaver, Peter D. "Blowback: Information Warfare and the Dynamics of Coercion." *Security Studies* 7, no. 4 (Summer 1998): 88-120.

Forseca, Brian. "$12.1 billion reportedly spent to ward off computer viruses in 1999." *CNN*, 18 January 2000, n.p. Online. Internet, 25 March 2000. Available from www.cnn.com/2000/TECH/computing/01/18/virus.cost.idg/index.html.

Frye, Major Dwayne W. "Information Warfare (IW): Air Staff Roles and Responsibilities." Research Report no. AU/ACSC/0603/97-03. Maxwell AFB, Ala.: Air Command and Staff College, March 1997.

"Joint Force Information Warfare Component Commander." *HQ USAF Doctrine Center--Doctrine Issues, Initiatives and Information*, Feb 00, n.p. Online. Internet, 25 March 00. Available from www.doctrine.af.mil/application/issues/jfiwcc.pdf.

Joint Publication 3-13. *Joint Doctrine for Information Operations.* 9 October 1998.

Keany, Thomas A. and Eliot A. Cohen. *Gulf War Air Power Survey Summary Report.* Washington, D.C.: U.S. Government Printing Office, 1993.

Khalilzad, Zalmay M., and John P. White, eds. *The Changing Role of Information in Warfare.* RAND Report MR-1016-AF. Santa Monica, Calif.: RAND, 1999.

Kosovo/Operation Allied Force After Action Report, Report to Congress, January 31, 2000.

Libicki, Martin and Jeremy Shapiro. "Conclusion: The Changing Role of Information in Warfare." In *The Changing Role of Information in Warfare.* RAND Report MR-1016-AF. Edited by Zalmay M. Khalilzad and John P. White. Santa Monica, Calif.: RAND, 1999.

Marsan, Carolyn Duffy. "Y2K figures hide hardware upgrades." *CNN*, 10 January 2000, n.p. Online. Internet, 22 March 2000. Available from www.cnn.com/2000/TECH/computing/01/10/y2k.budget.idg/index.html.

Peifer, Capt Kenneth V. "An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy." Research Report no. AU/AFIT/LAS/97D-10. Wright-Patterson AFB, Ohio: Air Force Institute of Technology, December 1997.

Rattray, Gregory J. "Strategic Information Warfare: Challenges for the United States." Research Report no. AU/AFIT/98-003D. Wright-Patterson AFB, Ohio: Air Force Institute of Technology, May 1998.

Rothrock, John. "Information Warfare: Time for Some Constructive Criticism?" In *In Athena's Camp: Preparing For Conflict In The Information Age.* RAND Report MR-880-OSD. Edited by John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND, 1997.

Schwartzstein, Stuart J.D., ed. *The Information Revolution and National Security: Dimensions and Directions.* Washington D.C.: The Center for Strategic and International Studies, 1996.

Seinwill, Major Jeffrey D. "Organizing for Information Operations: The Viability of a Joint Force Information Operations Component Commander." Research Report no. AU/ACSC/185/1999-04. Maxwell AFB, Ala.: Air Command and Staff College, April 1999.

Shapiro, Jeremy. "Information and War: Is it a Revolution?" In *The Changing Role of Information in Warfare.* RAND Report MR-1016-AF. Edited by Zalmay M. Khalilzad and John P. White. Santa Monica, Calif.: RAND, 1999.

Sundberg, Jared. "Why Y2K Won't Die." *Newsweek*, 10 January 2000, n.p. Online. Internet, 22 March 2000. Available from http://newsweek.com/nw-srv/printed/us/sr/a47027-2000jan2.htm.

Syrett, David. "Northwest Africa 1942-1943." In *Case Studies in the Achievement of Air Superiority.* Edited by Benjamin Franklin Cooling. Washington, D.C.: Center for Air Force History, 1994.

Szafranski, Richard. "Neocortical Warfare? The Acme of Skill." In *In Athena's Camp: Preparing For Conflict in the Information Age.* RAND Report MR-880-OSD. Edited by John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND, 1997.

Toffler, Alvin and Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little, Brown and Company, 1993.

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 1963.

van Creveld, Martin. *The Transformation of War*. New York: The Free Press, 1991.